

IN THE CLAIMS:

Please amend the claims as shown below ion the listing of claims.

Claims 1-6. (Cancelled)

7. (Previously presented) A method of operating a storage device, comprising:
detecting data integrity errors in the storage device;
counting each data integrity error in a count;
when the count reaches a threshold limit, placing the storage device into a forced
failure state;
returning the storage device from the forced failure state to an operational state,
wherein said returning the storage device from the forced failure state to
an operational state comprises decreasing the threshold limit for the
storage device after placing the storage device into a forced failure state;
and
setting the count to a base level.
8. (Previously presented) A method of operating a storage device, comprising:
detecting data integrity errors in the storage device;
counting each data integrity error in a count;
when the count reaches a threshold limit, placing the storage device into a forced
failure state;
returning the storage device from the forced failure state to an operational state,
wherein said returning the storage device from the forced failure state to
an operational state comprises increasing the base level after placing the
storage device into a forced failure state; and
setting the count to a base level.

Claims 9-12. (Cancelled)

13. (Currently amended) ~~The method of Claim 1, further comprising:~~

A method of operating a storage device, comprising:

detecting data integrity errors in the storage device;

counting each data integrity error in a count;

when the count reaches a threshold limit, placing the storage device into a forced failure state;

returning the storage device from the forced failure state to an operational state,

tracking the time elapsed after a first data integrity error; ~~and~~

decreasing the count if the time elapsed after the first data integrity error and

before a second data integrity error is greater than a preset refresh period;

and

setting the count to a base level.

Claims 14-22. (Cancelled)

23. (Previously presented) A storage system, comprising:

a storage device; and

a demerit monitor coupled to the storage device operable to:

detect data integrity errors in the storage device;

count each data integrity error in a count;

when the count reaches a threshold limit, place the storage device into a

forced failure state, wherein said demerit monitor decreases the

threshold limit for the storage device after placing the storage

device into a forced failure state;

return the storage device from the forced failure state to an operational

state; and

set the count to a base level.

24. (Previously presented) A storage system, comprising:

a storage device; and

a demerit monitor coupled to the storage device operable to:

detect data integrity errors in the storage device;
count each data integrity error in a count;
when the count reaches a threshold limit, place the storage device into a
forced failure state, wherein said demerit monitor increases the
base level after placing the storage device into a forced failure
state;
return the storage device from the forced failure state to an operational
state; and
set the count to a base level.

Claims 25-28. (Cancelled)

29. (Currently amended) ~~The storage system of Claim 15, wherein said demerit monitor tracks the time elapsed after a first data integrity error, and decreases the count if the time elapsed after the first data integrity error and before a second data integrity error is greater than a refresh period.~~
- A storage system, comprising:
a storage device; and
a demerit monitor coupled to the storage device operable to:
detect data integrity errors in the storage device;
count each data integrity error in a count;
track the time elapsed after a first data integrity error; and
decrease the count if the time elapsed after the first data integrity error and
before a second data integrity error is greater than a refresh period;
when the count reaches a threshold limit, place the storage device into a forced
failure state, return the storage device from the forced failure state to an
operational state; and
set the count to a base level.

Claims 30-36. (Cancelled)

37. (Previously presented) A computer-readable medium whose contents cause a computer system to operate a storage device, by performing the steps of:
detecting data integrity errors in the storage device;
counting each data integrity error in a count;
when the count reaches a threshold limit, placing the storage device into a forced failure state;
returning the storage device from the forced failure state to an operational state, wherein said returning the storage device from the forced failure state to an operational state comprises decreasing the threshold limit for the storage device after placing the storage device into a forced failure state;
and
setting the count to a base level.
38. (Previously presented) A computer-readable medium whose contents cause a computer system to operate a storage device, by performing the steps of:
detecting data integrity errors in the storage device;
counting each data integrity error in a count;
when the count reaches a threshold limit, placing the storage device into a forced failure state;
returning the storage device from the forced failure state to an operational state, wherein said returning the storage device from the forced failure state to an operational state comprises increasing the base level after placing the storage device into a forced failure state; and
setting the count to a base level.

Claims 39-42. (Cancelled)

43. (Currently amended) ~~The computer-readable medium of Claim 31, wherein the steps further comprise:~~
A computer-readable medium whose contents cause a computer system to operate a storage device, by performing the steps of:

detecting data integrity errors in the storage device;
counting each data integrity error in a count;
when the count reaches a threshold limit, placing the storage device into a forced
failure state;
returning the storage device from the forced failure state to an operational state;
tracking the time elapsed after a first data integrity error; ~~and~~
decreasing the count if the time elapsed after the first data integrity error and
before a second data integrity error is greater than a preset refresh period;
and
setting the count to a base level.

44. (Cancelled)